Privacy of Consumer Financial Information

Policy & Program

I. Purpose

The purpose of this policy is to ensure compliance with Gramm-Leach-Bliley Act (GLBA) information-sharing practices set forth by 12 CFR Part 1016 – Privacy of Consumer Financial Information within Tolomeo Bank International, Corp. This part applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes and is applicable to Tolomeo Bank International, Corp., as a financial institutions for which the Bureau of Consumer Financial Protection (Bureau) has rulemaking authority pursuant to section 504(a)(1)(A) of the Gramm-Leach-Bliley Act (GLB Act). This part requires financial institutions to provide each consumer with a written privacy policy notice at the time the consumer relationship is established and annually thereafter. The privacy notice must explain the information-sharing practices. The notice must also identify the consumer's right to opt out of the information being shared with unaffiliated parties pursuant to the provisions of the Fair Credit Reporting Act. The unaffiliated parties receiving the Non-Public Personal Identifiable Information (NPPII) are held to the acceptance terms of the consumer under the original relationship agreement. Also, this act requires financial institutions to develop a written information security plan describing its processes and procedures for protecting clients' Non-Public PII. GLBA Non-Public PII guidelines apply to any non-public information, which is defined as information a customer may provide to facilitate a transaction or which is otherwise obtained by the institution. As a covered entity, Tolomeo Bank International, Corp., must ensure compliance with this Policy & Program in order to construct a thorough understanding of each department handling the nonpublic information, as well as develop and monitor the program to secure the information. If there are changes in how information is collected, stored, and used, the safeguards must be updated as well. The Federal government provides a set of standards for safeguarding customer information. Complying with this Part ensures the effective management of change while reducing risk. Changes include, but are not limited to: improvements, updates, and maintenances, among others. All changes must be evaluated, planned and monitored in order to minimize any adverse impact to Tolomeo Bank International, Corp., operations.

II. Scope

The objective of this policy is to establish the general guidelines to ensure that Tolomeo Bank International, Corp., and their affiliates safeguard the confidentiality of personal identifiable information (PII) gathered from customer records in paper, electronic or other forms, in order to protect customers' privacy and securely protect their sensitive personal information against unauthorized access. This policy applies to all Tolomeo Bank International, Corp., personnel that collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle NPPII. This policy establishes the general guidelines for handling NPPII, in order to prevent and limit noncompliance with GLBA on Tolomeo Bank International, Corp.'s, daily operations.

Non-Public PII includes, but is not limited to, any information an individual gives you to get a financial product or service (for example, name, address, income, Social Security number, Passport/VISA/Government identification number or other information on an application), any information you get about an individual from a transaction involving your financial product(s) or service(s) (for example, the fact that an individual is your consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases), or any information you get about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report). PII does not include information that you have a reasonable basis to believe is lawfully made «publicly available.» In other words, information is not NPPII when you have taken steps to determine that the information is generally made lawfully available to the public and that the individual can direct that it not be made public and has not done so. Publicly Available information includes, but is not limited to, federal, state, or local government records made available to the public, such as information that is widely distributed through media like telephone books, newspapers, and websites that are available to the general public on an unrestricted basis, even if the site requires a password or fee for access.

III. Definitions

- ***Affiliate*:** In any company that controls, is controlled by, or is under common control with Tolomeo Bank International, Corp.
- ***Consumer*:** Is an individual or that individual's legal representative, who obtains or has obtained a financial product or service from Tolomeo Bank International, Corp., that is to be used primarily for personal, family, or household purposes.
- ***Customer*:** Is a consumer who has a continuing relationship between a consumer and Tolomeo Bank International, Corp., under which Tolomeo Bank International, Corp., provides one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes.

- ***Financial service*:** Includes, among other things, Tolomeo Bank International, Corp.'s evaluation, assistance or brokerage of information that is collated in connection with a request or an application from a consumer for a financial product or service.
- ***Nonaffiliated third party:*** Is any person except Tolomeo Bank International, Corp.'s affiliate or a person employed jointly by

Tolomeo Bank International, Corp., and a company that is not the bank's affiliate.

- ***Non-Public Personal Identification Information (NPPII)*:** Is any information that is not publicly available and that a consumer provided to Tolomeo Bank International, Corp., to obtain a financial product or service from the institution and/or results from a transaction between the consumer and Tolomeo Bank International, Corp., that involves a financial product or service obtained otherwise about a consumer in connection with providing a financial product or service.
- ***Opt Out*:** The right provided to customers and/or consumers to discontinue the sharing of his/her

NPPII with a nonaffiliated third party.

IV. Policy

Safeguards Over Information

– Tolomeo Bank International, Corp., protects customer information to achieve confidentiality, integrity and availability. Confidentiality means that NPPII is not available or disclosed to unauthorized persons. Integrity means that NPPII is not altered/destroyed in an unauthorized manner. Availability means that NPPII is accessible and usable on demand by an authorized person.

– Tolomeo Bank International, Corp., attains administrative safeguards by implementing security measures that reduce risks/vulnerabilities to a reasonable and appropriate level.

– Tolomeo Bank International, Corp., achieves physical safeguards by limiting physical access to its facilities while ensuring that authorized access is allowed and follows the appropriate procedures established.

– Tolomeo Bank International, Corp., achieves technical safeguards by implementing technical policies and procedures that allow only authorized users to access

electronic NPPII. Electronic measures must be put in place to confirm that NPPII has not been improperly altered or destroyed.

– Tolomeo Bank International, Corp., will achieve organizational safeguards by taking reasonable steps to cure any activity or practice that constitutes a material breach or violation. Violations include the failure to implement safeguards that reasonably and appropriately protect NPPII.

– Tolomeo Bank International, Corp., will adopt reasonable and appropriate procedures to comply with this Policy. Tolomeo Bank International, Corp., must maintain written security procedures and written records of required actions, activities or assessments.

– Tolomeo Bank International, Corp., must perform a risk assessment if a breach occurs to evaluate the probability of that the protected information has been compromised.

Information

Requirements for Notices

– Privacy notices must be clear and conspicuous and must accurately reflect the institution's privacy practices.

– The privacy notice will be provided so that each recipient can reasonably be expected to receive actual notice in writing or electronically.

– Privacy notices will be available on the website of Tolomeo Bank International, Corp.

– The privacy notice includes the following information:

- Categories of information collected,
- Categories of information disclosed,
- Categories of affiliates and nonaffiliated third parties to whom Tolomeo Bank International, Corp., may disclose information,
- Policies and practices concerning the treatment of former customers' information,
- Categories of information disclosed to nonaffiliated third parties that perform services for Tolomeo Bank International, Corp., or functions on Tolomeo Bank International, Corp.'s behalf and categories of third parties with whom Tolomeo Bank International, Corp. has contracted,
- An explanation of the opt-out right and methods for opting out, Policies and practices for protecting the security and confidentiality of information, and

- A statement that Tolomeo Bank International, Corp., makes disclosures to other nonaffiliated third parties for everyday business purposes or as permitted by the law.

Notice Duties to Customers

– Tolomeo Bank International, Corp., will provide an initial notice of its privacy policies and practices to each customer, no later than the time a customer relationship is established.

– Gramm-Leach-Bliley Act (GLBA) gives rule making authority to the CFPB and modifies Regulation P on the requirements of Annual Notice indicating that "the institutions are not required to deliver an annual privacy notice if: (i) Provide nonpublic personal information to nonaffiliated third parties only in accordance with the provisions of § 1016.13, § 1016.14, or § 1016.15; and (ii) Have not changed their policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed to the customer under § 1016.6(a)(2) through (5) and (9) in the most recent privacy notice provided pursuant to this part."

Therefore, it is the policy of Tolomeo Bank International, Corp., to provide the ongoing annual Privacy Notice to existing customers only if at any giving point in time a change in policies and/or practices occurs in regards to disclosing nonpublic personal information from the policies and practices that were disclosed to the customer under § 1016.6(a)(2) through (5) and (9) in the most recent privacy notice provided pursuant to this part.

– A new notice will be provided to an existing customer when the customer obtains a new financial product or services, only if the initial or annual notice most recently provided to the customer was not accurate with respect to the financial product or service.

Information to be collected from Customers when Opening a New Account

– Tolomeo Bank International, Corp., will notify the customers of new account the requirement of the following information: his/her name, address, date of birth, profession, origin of income, and any other information that will allow the identification of the customer. This applies to both, deposits and credit accounts, and any other type of account offered by Tolomeo Bank International, Corp.

– Tolomeo Bank International, Corp., might also request the license ID, Passport or any other identification documents to the customer or representative, if applicable.

– Tolomeo Bank International, Corp., will notify that they will reserve the right of requesting additional documents to the accounts primary signature, authorized signatures, and/or origin of funds reflected on the account, and/or customers' income.

– Tolomeo Bank International, Corp., will notify that the client is not required to accept the disclaimers when opening a new account. If clients are not in agreement with the disclaimers, Tolomeo Bank International, Corp., will close the new account and return the available funds by Check or via wire transfer without any cost to the client.

– Information about the devices from which the customer access our account origination platform and other data captured automatically (such as operating system type, mobile device brand and model, IP address, settings, and downloaded applications).

– Information about customer location (geolocation), primarily used to confirm that you are within the coverage area to offer you services, among other purposes.

– List of contacts and installed apps from mobile devices to validate the customer identity, prevent digital fraud, and verify the customer profile. Information we Collect from Other Sources.

– Information collected for fraud prevention purposes and compliance with reporting requirements.

– Data used for identity validation, information completion, or correction, obtained from secure and reliable sources such as public agencies, service providers, or business partners with whom we collaborate.

Opt Out Duties to Consumers

– Tolomeo Bank International, Corp., will send an initial notice of its privacy policies and practices via e-mail, providing this is the official method of communication, as all customers must agree.

– The information sent to the consumer will include an opt-out notice.

– The opt-out notice will allow a period of no less than 30 days for the consumer to opt-out.

– Tolomeo Bank International, Corp., will notify its new clients that their account or transaction information could be disclosed in the following scenarios:

- Verification of existence and condition of clients account to third party (e.g. credit bureau, merchants)

- Complying with warrants made from courts or governmental agencies,
- When required in order to process or complete a transaction, ● When the customer authorizes in writing, and
- When required or permitted by legislation and applicable laws.

– Tolomeo Bank International, Corp., will not disclose any nonpublic personal information to non-affiliated third parties except under the enumerated exceptions.

– Tolomeo Bank International, Corp., will provide a revised notice before it begins to share a new category of nonpublic personal information or shares information with a new category of nonaffiliated third party in a manner that was not described in the previous notice.

Monitoring of Compliance

– Tolomeo Bank International, Corp., has designated an officer that is not involved in the proper execution of this policy, the task of monitoring the proper compliance of this policy and/or pertinent procedure.

– Action plans and/or corrective measures will be documented, approved and distributed within the affected area and management.

– The areas to be evaluated are:

- Initial privacy notice,
- Annual privacy notice (if considered applicable),
- Content privacy notice,
- No Opt-out notice,
- Revised notice,
- Delivery methods,
- Limits on disclosure to nonaffiliated third parties,
- Limits on disclosure and reuse of information,
- Roles and Responsibilities
- Exceptions to notice and opt-out requirements for processing servicing transactions, and
- Other exceptions to notice and opt-out requirements.

Response Program for Unauthorized Access to Customer

– Tolomeo Bank International, Corp., has in place a risk-based response, including customer notification procedures, to address unauthorized access to or use of

customer information maintained by Tolomeo Bank International, Corp., or its service provider that could result in substantial harm or inconvenience to any customer, and require disclosure of a data security breach if the covered entity concludes that misuse of its information about a customer has occurred or is reasonably possible, pursuant to the guidance, substantial harm or inconvenience is most likely to result from improper access to “sensitive customer information”.

– Tolomeo Bank International, Corp’s response program general procedures are:

- Assessing through an investigation the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused; assessing the situation could include the support of a third party, as considered necessary.
- Notifying its primary regulators once Tolomeo Bank International, Corp., becomes aware of an incident involving unauthorized access to or use of
- sensitive customer information; consistent with the Agency’s Suspicious Activity Report (“SAR”) regulations,
- Notifying appropriate law enforcement authorities;
- Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer
- information (e.g., by monitoring, freezing, or closing affected accounts and preserving records and other evidence); and
- Notifying the affected customers when warranted. Customer notice may only be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay.

– Tolomeo Bank International, Corp., has an affirmative duty to protect their customers’ information against unauthorized access or use, and customer notification of a security breach involving the customers’ information is a key part of that duty.

Breach Notification Contents

– The contents of a breach notification should contain the following elements:

- A general description of the incident,
- Type of information subject to unauthorized access,
- A telephone number customers can call for further information and assistance,
- A reminder «to remain vigilant» over the next 12 to 24 months,
- A recommendation that incidents of suspected identity theft be reported promptly, and
- A general description of the steps taken by the financial institution to protect the information from further unauthorized access or use.

- Depending on the situation, Tolomeo Bank International, Corp., may choose to contact all customers affected by telephone or by electronic mail.

Suspicious Activity Report ("SAR")

– Tolomeo Bank International, Corp., is required to file a suspicious activity report no later than 30 calendar days after the date of initial detection of unusual facts that may constitute a basis for filing a suspicious activity report.

– If no suspect was identified on the date of detection of the incident requiring the filing, Tolomeo Bank International, Corp., may delay filing a suspicious activity report for an additional 30 calendar days to identify a suspect.

– In no case shall reporting be delayed more than 60 calendar days after the date of initial detection of a reportable transaction.

– Tolomeo Bank International, Corp., must use the regular channels in order to submit Suspicious Activity Reports.

Amendments

This program/policy is subject to review and revision to ensure compliance with current and future laws and regulations. With the exception of modifications, supplements or updates necessitated by changes in law, regulations or administrative requirements, or to ensure consistency with other Bank policies, any proposed amendments to this Policy must be approved by Tolomeo Bank International, Corp.'s Board of Directors.

Validity

This policy will take effect on the effective date (approval date) established by the document. It is provided that new procedures adopted in this policy must be integrated to Tolomeo Bank International, Corp.'s operation in a term no longer than 90 days from the effective day. Human Resources will be responsible for the notification to Tolomeo Bank International's employees' prior its implementation and the notification of any changes the policy suffers after the effective date. Any employee who does not comply with the established norms- could be reprimanded according to the progressive discipline process.